

ASA クライアントレス SSLVPN : RDP プラグインの問題

内容

[概要](#)

[背景説明](#)

[Java プラグイン](#)

[Active-X プラグイン](#)

[RDP プラグイン](#)

[RDP と RDP-2 プラグインの使用](#)

[ActiveX クライアントと Java クライアントの位置付け](#)

[RDP-ActiveX](#)

[RDP-Java](#)

[RDP ブックマークの形式](#)

[RDP プラグインおよび VPN ロードバランシング](#)

[FAQ](#)

[入力した文字の一部がリモート RDP セッションで表示されないのはどうしてですか。](#)

[キーボード マッピングの既知の問題](#)

[Java RDP プラグインは全画面の RDP セッションをサポートしていますか。](#)

[Java クライアントは暗号化に AES-256 を使用して通信できますか。](#)

[RDP 問題のトラブルシューティング](#)

[既知の注意事項](#)

[Microsoft セキュリティ更新プログラムに関連する問題](#)

[ActiveX Client](#)

[Java Client](#)

概要

このドキュメントは、Remote Desktop Protocol (RDP) プラグインに関してよく寄せられる質問 (FAQ) のいくつかに回答します。RDP プラグインは、Cisco 適応型セキュリティ アプライアンス (ASA) のクライアントレス セキュア ソケット レイヤ VPN (SSLVPN) ユーザが利用できるプラグインです。

RDP プラグインは、ユーザが利用できるプラグインの 1 つで、セキュア シェル (SSH)、Virtual Network Computing (VNC)、Citrix などと同様です。RDP プラグインは、それらの中で最もよく使用されるプラグインの 1 つです。このドキュメントは、導入の詳細と、このプラグインに対するトラブルシューティング手順について説明します。

注：このドキュメントでは、RDP プラグインの設定方法は説明していません。詳細については、[Cisco ASA 5500 SSL VPN 導入ガイド、バージョン 8.x](#) を参照してください。

背景説明

RDP プラグインは、ピュア Java ベースの RDP プラグインから進化したもので、ActiveX RDP クライアント (Internet Explorer) と Java クライアント (Internet Explorer 以外のブラウザ) の両方に対応しています。

Java プラグイン

Java RDP クライアントは、[Proper Java RDP アプレットを使用します](#)。Java アプレットは ASA クライアントレス ポータルにインストール可能なプラグインにラップされています。

Active-X プラグイン

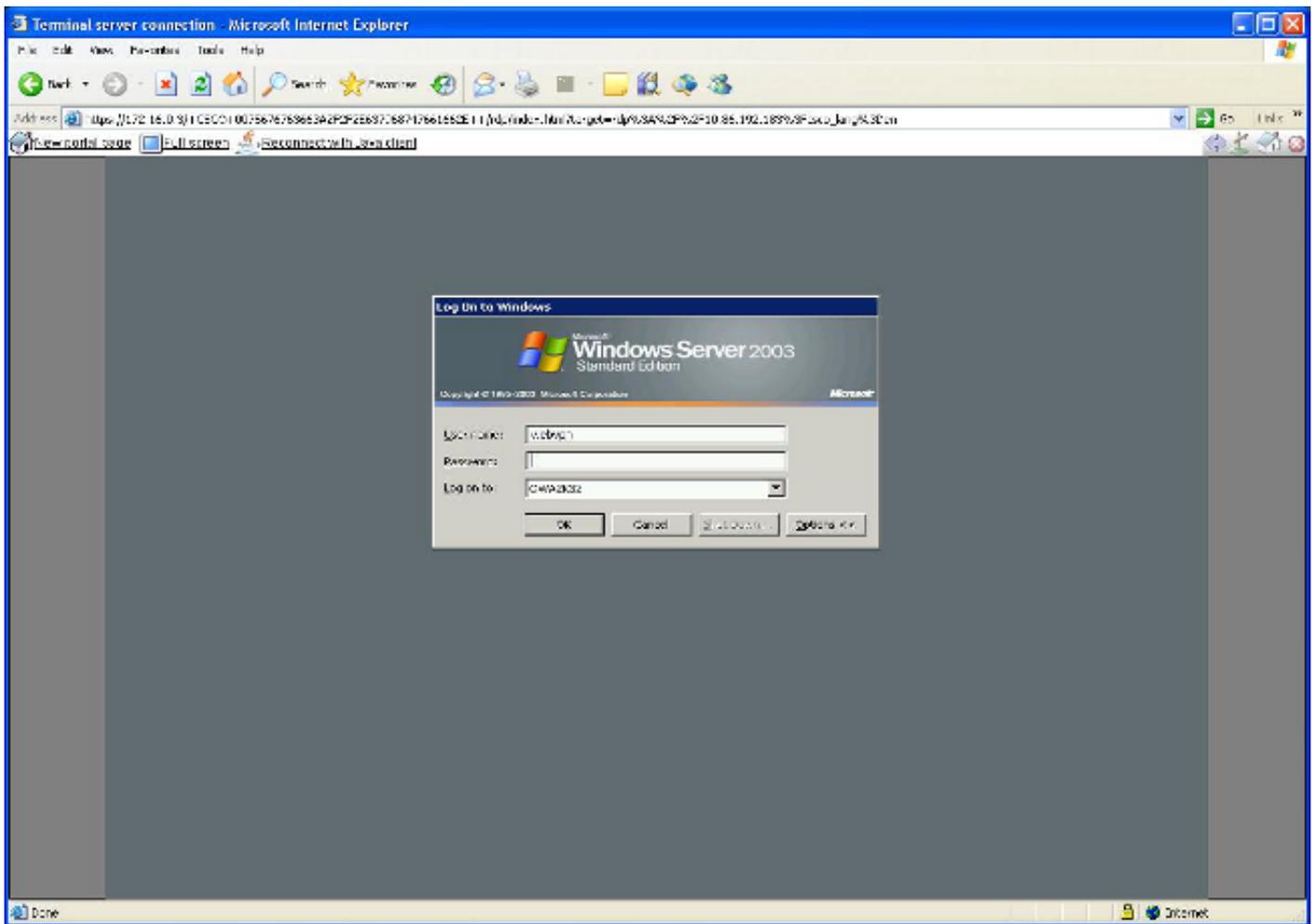
RDP プラグインには Microsoft ActiveX RDP クライアントも含まれ、プラグインはブラウザによって Java クライアントと ActiveX クライアントのどちらを使用するかを判断します。つまり、次のようになります。

- Internet Explorer(IE)ユーザーがクライアントレスSSLVPNポータルを介してRDPを使用しようとし、ブックマークURLにForceJava=true引数が含まれていない場合は、ActiveXクライアントが使用されます。ActiveXの実行が失敗場合、プラグインはJavaクライアントをを開始します。
- IE 以外のユーザが RDP ブックマークまたは URL を起動しようとする、起動されるのは Java クライアントだけです。

RDP ActiveX およびユーザ権限の要件の詳細については、Microsoft の記事、[Requirements for Remote Desktop Web Connection](#) を参照してください。

次の画像は、プラグインが起動した後、ブラウザ ウィンドウ内で選択できる 3 つのリンクを示しています。

1. [New Portal Page] : このリンクは、新しいブラウザ ウィンドウにポータル ページを開きます。
2. [Full-Screen] : RDP ウィンドウを全画面モードで使用します。
3. [Reconnect with Java] : 意図的にプラグインに再接続して、ActiveX の代わりに Java を使用します。



RDP プラグイン

RDP と RDP-2 プラグインの使用

- RDPプラグイン：これは、JavaクライアントとActiveXクライアントの両方を含むオリジナルのプラグインです。
- RDP2プラグイン：RDPプロトコルの変更により、Proper Java RDP Clientが更新され、Microsoft Windows 2003ターミナルサーバおよびWindows Vistaターミナルサーバがサポートされるようになりました。

ヒント：最新の RDP プラグインは RDP と RDP2 の両方のプロトコルを統合しています。その結果、RDP2 プラグインが廃止されています。最新のバージョンの RDP プラグインを使用することをお勧めします。RDPプラグインの名称は`rdp-plugin.yymmdd.jar`の構造に従います。ここで、`yy`は2桁の年形式、`mm`は2桁の月形式、`dd`は2桁の日形式です。

プラグインをダウンロードするには、シスコの[ソフトウェアダウンロード](#)のページにアクセスしてください。

Worldwide [change] | Welcome, Aki Bessu | Account | Log Out | My Cisco

Products & Services | Support | How to Buy | Training & Events | Partners

Download Software

Download Cart (2 items) | Feedback | Help

Downloads Home > Products > Security > Firewalls > Firewall Appliances > Cisco ASA 5500 Series Adaptive Security Appliances > Cisco ASA 5520 Adaptive Security Appliance > Remote Access Plugins for Adaptive Security Appliance (ASA)-1.1.1

Cisco ASA 5520 Adaptive Security Appliance

Search... | Expand All | Collapse All

All Releases

- 1.1.1
- 1.0.0

Release 1.1.1

File Information	Release Date	Size	
Terminal Service client plugin for ASA. rdp-plugin.120424.jar	27-APR-2012	0.86 MB	Download Add to cart Publish
Citrix (do-it-yourself) client plugin for ASA. ica-plugin.04.23.2012.zip	24-APR-2012	0.01 MB	Download Add to cart Publish
Cisco plugin for Siteminder Policy Server to enable ASA SSO support via Siteminder. cisco_vpn_auth.jar	15-FEB-2008	0.01 MB	Download Add to cart Publish
Citrix (do-it-yourself) client plugin for ASA. ica-plugin.100805.zip	15-FEB-2008	0.01 MB	Download Add to cart Publish
HTTP POST request plugin for ASA. post-plugin.090722.jar	15-FEB-2008	0.05 MB	Download Add to cart

ActiveX クライアントと Java クライアントの位置付け

RDP-ActiveX

- IE でのみ使用。
- 音声の転送をサポート。

RDP-Java

- Java が有効なすべてのサポート対象のブラウザで機能。
- ActiveX の起動が失敗するか、RDP ブックマーク内で ForceJava=true 引数が渡された場合にのみ IE で Java クライアントが起動。
- RDP Java の実装は、オープンソース イニシアチブの Proper Java RDP プロジェクトに基づく。アプリケーションのサポートは、ベスト エフォート。

RDP ブックマークの形式

RDP のブックマークの形式の例を示します。

```
rdp://server:port/?Parameter1=value&Parameter2=value&Parameter3=value
```

形式に関する重要な点は次のとおりです。

- **server** : これは唯一必須の属性です。Microsoft Terminal Service をホストするコンピュータの名前を入力します。
- **port (オプション)** : これは、Microsoft Terminal Service をホストするリモート コンピュータ内の仮想アドレスです。デフォルト値は 3389 で、Microsoft Terminal Service のウェルノウン ポート番号と同じです。
- **parameters** : これはパラメータと値のペアで構成されるオプションのクエリ文字列です。疑問符は引数の文字列の始まりを示し、各パラメータと値のペアはアンパサンドで区切られます。

使用可能なパラメータのリストを以下に示します。

geometry : クライアント画面のサイズ (幅 × 高さ、ピクセル)。 **bpp** : ビットパーピクセル (カラー深度) 8、16、24、32。 **domain** : ログインドメイン。 **username** : ログイン ユーザー名。 **password** : ログイン パスワード。パスワードはクライアント側で使用され、見えてしまうので、使用には注意してください。 **console** : サーバ上のコンソール セッションに接続するために使用します (yes/no)。 **ForceJava** : Java クライアントだけを使用するには、このパラメータを yes に設定します。デフォルト設定は no です。 **shell** : RDP で接続した際に自動的に開始される実行可能ファイルやアプリケーションのパスを設定します (例 : rdp://server/?shell=path)。

次に、ActiveX 専用の追加のパラメータの一覧を示します。

RedirectDrives : リモート ドライブをローカルにマップするには、このパラメータを true に設定します。 **RedirectPrinters** : リモート プリンタをローカルにマップするには、このパラメータを true に設定します。 **FullScreen** : 全画面モードで起動するにはこのパラメータを true に設定します。 **ForceJava** : Java クライアントを意図的に使用するには、このパラメータを yes に設定します。 **audio** : このパラメータは、RDP セッションを介した音声転送に使用されます。

0 : リモート音声をクライアント コンピュータにリダイレクトします。 1 : リモート コンピュータで音声を再生します。 2 : 音声のリダイレクトを無効にします。リモート サーバで音声は再生されません。

RDP プラグインおよび VPN ロードバランシング

複数の拠点間でのロードバランシングが、ドメイン ネーム サーバ (DNS) ベースの [Global Server Load Balancing \(GSLB; グローバル サーバ ロードバランシング \)](#) でサポートされています。DNS の結果のキャッシュの違いにより、プラグインの動作はオペレーティング システムによって異なる場合があります。Windows DNS のキャッシュでは、プラグインが Java アプレットを起動すると同じ IP アドレスを解決できます。Macintosh (Mac) OS X では、Java アプレットが異なる IP アドレスを解決する場合があります。その結果、プラグインは正しく起動しません。

DNS ラウンドロビンの例は、1 つの URL (<https://www.example.com>) で、www.example.com に対する DNS エントリが 192.0.2.10 (ASA1) または 198.51.100.50 (ASA2) のいずれかで解決できる場合です。

ユーザが ASA1 上のブラウザからクライアントレス WebVPN ポータルにログインすれば、RDP

プラグインを開始できません。Java クライアントの起動中に、MAC OS X のコンピュータは新しい DNS 解決要求を実行します。ラウンドロビン DNS の設定では、2 番目の解決要求に対する応答で、最初の WebVPN 接続で選択されたものと同じサイトに戻る確率は 50 % です。DNS サーバの応答が 192.0.2.10 (ASA1) ではなく 198.51.100.50 (ASA2) の場合、Java クライアントは誤った ASA (ASA2) への接続を開始します。ユーザ セッションが ASA2 には存在しないため、接続要求は拒否されます。

その結果次のような Java エラー メッセージが表示される場合があります。

```
java.lang.ClassFormatError: Incompatible magic value 1008813135 in
class file net/propero/rdp/applet/RdpApplet
```

FAQ

入力した文字の一部がリモート RDP セッションで表示されないのはどうしてですか。

RDP セッションでリモート コンピュータのキーボードのリージョン設定がローカル コンピュータと異なる場合があります。この違いにより、リモートコンピュータでは入力された特定の文字や間違った文字が表示されない可能性があります。この動作は、Javaプラグインでのみ発生します。この問題を解決するには、**keymap** 属性を使用して、ローカルのキーマップをリモート PC にマッピングします。

たとえば、ドイツ語のキーボード マップを設定するには、次のように使用します。

```
rdp://
```

The following keymaps are available:

```
-----
ar   de   en-us fi   fr-be it   lt   mk   pl   pt-br sl   tk
da   en-gb es   fr   hr   ja   lv   no   pt   ru   sv   tr
-----
```

キーボード マッピングの既知の問題

- Cisco Bug ID CSCth38454 : RDP プラグインへのハンガリー語のキーマップの実装
- Cisco Bug ID CSCsu77600 : WebVPN RDP プラグイン ウィンドウ キーが不正Shift (key) .jar。
- Cisco Bug ID CSCtt04614 : RDP プラグインで WebVPN - ES キーボード分音記号の管理が不正
- Cisco Bug ID CSCtb07767 : ASA プラグイン - デフォルトのパラメータの設定。

ヒント : 別の回避策として、**mstsc.exe**にアプリケーションスマートトンネルを使用する方

法があります。これはWebVPNのサブ設定モードでsmart-tunnel list RDP_List RDP mstsc.exe platform windowsコマンドで設定されます。

Java RDP プラグインは全画面の RDP セッションをサポートしていますか。

現在、RDP セッションの全画面モードはネイティブにはサポートされていません。実装するために、拡張要求 CSCto87451 が発行されています。geometry パラメータ (たとえば geometry =1024x768) がユーザのモニタの解像度に設定されたら、全画面モードで機能します。ユーザの画面サイズは異なるため、複数のブックマークリンクの作成が必要となる場合があります。ActiveX クライアントは、全画面 RDP セッションをネイティブにサポートします。

Java クライアントは暗号化に AES-256 を使用して通信できますか。

Java クライアントが SSL を正しくネゴシエートできるようにするには、次のように ASA SSL 暗号セットの順序を調整してください。

```
Enabled cipher order: aes256-sha1 rc4-sha1 aes128-sha1 3des-sha1  
Disabled ciphers: des-sha1 rc4-md5 null-sha1
```

Java クライアントは、暗号セットの順序が異なると、このエラーを表示する場合があります。

```
[Thread-12] INFO net.propero.rdp.Rdp - javax.net.ssl.SSLHandshakeException:  
Received fatal alert: handshake_failure
```

RDP 問題のトラブルシューティング

RDP プラグインで別の問題が発生する場合、RDP の問題をトラブルシューティングするために次のデータを収集すると役立つ可能性があります。

- ASA での show tech コマンドの出力
- ASA での show import webvpn plug-in detailed コマンドの出力
- ユーザ コンピュータのオペレーティング システムおよびパッチ レベル
- 宛先コンピュータのオペレーティング システムおよびパッチ レベル
- 使用されるクライアント (ActiveX または Java) および Java JRE のバージョン
- ASA がロードバランス クラスタ内にあるか、DNS ベースか、それとも ASA ベースかの確認

既知の注意事項

Microsoft セキュリティ更新プログラムに関連する問題

1. [KB2695962 : Microsoft Security Advisory](#)ActiveX の Kill Bit 更新プログラムのロールアップ : 2012 年 5 月 8 日。
2. [KB2675157 : MS12-023](#) : Internet Explorer 用の累積的なセキュリティ更新プログラム : 2012 年 4 月 10 日。

3. [cisco-sa-20120314-asaclient](#) : Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンス クライアントレス VPN ActiveX コントロール リモート コード実行脆弱性 3 月 14 日。
4. Cisco Bug ID CSCtx68075 : Windows Patch KB2585542 が適用される場合の ASA WebVPN の障害 (8.2.5.29/8.4.3.9) 。
5. [KB2585542 : MS12-006](#)。Windows の Webio、Winhttp、および schannel のセキュリティ更新プログラムの説明。2012 年 1 月 10 日。

ActiveX Client

- **症状** : ASA OS バージョン 8.4.3 へのアップグレード後、ActiveX クライアントが IE バージョン 6 ~ 9 でロードできない。

Cisco Bug ID [CSCtx58556](#)を参照してください。この修正は、バージョン8.4.3.4以降で利用できます。回避策 : 強制的に Java クライアントを使用します。

- **症状** : ActiveX Clientは、ASA OSバージョンが8.4.3より前のバージョンにダウングレードされた後でロードに失敗します。これは、Cisco Bug ID CSCtx58556の修正でASA上のActiveXクライアントを使用し、8.4.3より前のバージョンに接続しますx ASAバージョン8.4.3で導入されたRDPプラグイン。以前のバージョンとの互換性はありません。

Cisco Bug ID CSCtx57453 を参照してください。b8e73359-3422-4384-8d27-4ea1b4c01232? の Windows レジストリ インスタンスをすべて削除します (古い ActiveX CLSID) 。

注 : 編集する前にコンピュータ システム レジストリのバックアップを取ることをお勧めします。

- **症状** : ネットワーク レベル認証 (NLA) が有効になっているデバイスへ RDP 接続できない。

NLA が ActiveX RDP プラグインに統合されるようリクエストする拡張要求については Cisco Bug ID [CSCtu63661](#) を参照してください。Microsoft ActiveX のクライアントは NLA をサポートしますが、ASA プラグイン内でのその機能の使用はサポートされていません。回避策 : RDPプラグイン(mstsc.exe)をスマートトンネルに設定します。『[Cisco ASA 5500 SSL VPN導入ガイド、バージョン8.x](#)』を参照してください。

- **症状** : ActiveX RDP がロードされず、空白ページが表示される。

Cisco Bug ID [CSCsx49794](#) を参照してください。これは、ASA SSL 証明書の証明書チェーンが 4 つの証明書 (たとえば、ROOT、SUBCA1、SUBCA2、および ASA CERT) より大きい場合に発生します。回避策 :

ASA には大きい証明書チェーンをインストールしないでください。Java RDP プラグインは、ActiveX プラグインとは対照的に適切に機能することがわかっています。RDP は、Windows ネイティブ mstsc.exe をスマート トンネルで設定しても正しく機能します。

- **症状** : ActiveX RDP クライアントが使用された後、ユーザが [Logout] ボタンをクリックすると、HTTP 404 - Page Not found エラーが表示される。Cisco Bug ID CSCtz33266を参照してください。この問題は、プラグインバージョンrdp-plugin.120424.jar以降で解決されています

- 。
- **症状** : ユーザが IE を起動するとタブが 2 つ開き、1 つは RDP セッション、もう 1 つは空白ページ、または他の Web ページが表示される。[RDP] タブを閉じると IE が正しく機能しない。

Cisco Bug ID [CSCua69129](#) を参照してください。回避策 : Java RDP のプラグインを使用します (`ForceJava=true` を設定します) 。

- **症状** : ActiveX プラグインにより IE の CPU 使用率が高くなる。Cisco Bug ID [CSCua16597](#) を参照してください。
- **症状** : Windows アップデート KB2695962 のインストール後、ActiveX RDP プラグインがロードしない。新規 RDP セッションを開くと、ActiveX クライアントは Cisco SSL VPN Port Forwarder をインストールしようとし (これは常に発生するわけではありません)、リモートコンピュータに接続せずにクライアントレス ポータル ページを返します。これは脆弱性 CVE-2012-0358 によるもので、[Microsoft Security Advisory \(2695962 \)](#) によってクライアント側で解決されています。

Cisco Security Advisory の[Cisco ASA 5500 シリーズ適応型セキュリティアプライアンス クライアントレス VPN ActiveX コントロールのリモート コード実行の脆弱性](#)を参照してください。Cisco Bug ID [CSCtr00165](#) を参照してください。

Java Client

注:シスコは変更を加えずにプラグインを再配布します。GNU 一般公的使用許諾に基づき、シスコはプラグイン アプリケーションの変更や拡張を行いません。properJavaRDP プラグインは、オープン ソース アプリケーションであり、プラグイン ソフトウェアの問題はプロジェクト オーナーによって対処される必要があります。

- **症状** : Java RDP クライアントからアクセスされた場合に、プロセッサに負荷がかかるアプリケーションがリモート コンピュータで実行されると、Java アプレットがクラッシュする。

次のエラーメッセージが表示される可能性があります : `FATAL net.propero.rdp - javax.net.ssl.SSLException:Connection has been shutdown:....`この現象は、プロセッサに負荷がかかるアプリケーションを 2 つ以上短時間で切り替えると発生します。この問題は、プラグイン バージョン rdp.2012.6.4.jar 以降で修正されています。回避策 :

ActiveX クライアントを使用して接続します。アプリケーションを短時間で切替えないようにします。

- **症状** : Java RDPクライアントが次のエラーメッセージを生成します : `net.propo.rdp.Rdp - java.net.SocketException:Socket is closed java.net.SocketException:Socket is closed, and then closes.`

この問題は、FQDN (たとえば、`http://www.example.com`) だけでグループ URL が設定されたトンネル グループが原因で発生します。Cisco Bug ID [CSCuh72888](#) を参照してください。

回避策：

トンネルグループから「/」がないグループ URL エントリを削除します。ActiveX クライアントを使用します。

- **症状**：Java RDP クライアントが、Windows 8 のコンピュータに接続できない。

Java RDP クライアントは現在、Windows 8 をサポートしていません。Cisco Bug ID CSCuc79990 を参照してください。回避策：

ActiveX RDP クライアントを使用します。Windows ネイティブ RDP クライアントにスマートトンネルを適用します (`mstsc.exe`)。

- **症状**：Java RDPクライアントが次のエラーメッセージで失敗します。
ARSigningException:リソースで署名されていないエントリが見つかりました
： `https://10.105.130.91/+CSCO+3a75676763663A2F2F2E637968747661662E++/vnc/VncViewer.jar`

この問題は、ASA WebVPN Javaリライタのバグが原因で発生します。Cisco Bug ID [CSCuj88114](#)を参照してください。回避策：Javaバージョン7u40にダウングレードします。